UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

MATTHEW FERO, SHIRLEY KRENZER, ERIN O'BRIEN, individually and on behalf of all others similarly situated, Plaintiffs, v. EXCELLUS HEALTH PLAN, INC. and LIFETIME HEALTHCARE, INC. , Defendants.	Case No. 6:15-cv-06569 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

INTRODUCTION

1. Every business that collects and stores sensitive information about its customers has a duty to safeguard that information and ensure it is secure and remains private. That responsibility is most important where a business keeps and stores highly personal data such as the Social Security numbers, medical, and financial information belonging to its customers, and where the business retains such information about minor customers.

2. The data collected and stored by health insurance companies are among the most highly sensitive personally identifiable information. Health insurance companies, in turn, bear the crucial responsibility to protect this data from compromise and theft.

3. The threat of compromise is significant. In the past several years, cyberattacks have occurred across all industries with increasing frequency. In 2014 alone,

over one billion personal data records were compromised by cyberattack.[1] The healthcare and health insurance industries have not been exempt from these attacks. Indeed, the Ponemon Institute, an independent cyber security research institution, has reported that approximately 90% of health care organizations reported that they were the victims of at least one data breach over the past two years.[2] Similarly, a 2014 report by the Identity Theft Resource Center warned that the medical and healthcare industry accounted for 42.5% of all data breaches in 2014.[3] The risk of cyberattack is known and undeniable; it is imperative that healthcare and health insurance companies assume a corresponding duty to guard against this known risk and thwart preventable attacks.

4. Defendant Excellus Health Plan, Inc. ("Excellus") and defendant Lifetime Healthcare, Inc. ("Lifetime") comprise one of the largest health insurance companies in New York State. They insure almost two million individuals in upstate New York alone. Defendants also works closely with several affiliates, including Lifetime Benefit Solutions, Lifetime Care, Lifetime Health Medical Group, The MedAmerica Companies, and Univera Healthcare. Defendants maintain a massive amount of personally identifiable information on its past and current insureds, as well as those who have treated in its networks and have a duty to take all reasonable measures to protect this information and safeguard it from theft.

---

[1] CNBC, Year of the hack? A billion records compromised in 2014, http://www.cnbc.com/id/102420088# (last visited Sept. 16 2015).

[2] *See* Ponemon Institute LLC, Fourth Annual Benchmark Study on Patient Privacy & Data Security 2 (Mar. 2014), http://www.ponemon.org/local/upload/file/ID%20ExpertsPatient%20Privacy%20%26%20Data%20Security%20Report%20FINAL1-1.pdf.

[3] Identity Theft Resource Center, Data Breach Reports (Dec. 31, 2014), http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf.

5. This lawsuit arises from Defendants' failure to fulfill their legal duty to protect the sensitive information of their customers and those customers whose data was stored in its systems. On August 5, 2015, Defendants acknowledged that their system had been breached and the personal information of over 10 million policyholders had been compromised. Thieves potentially stole, *inter alia*, customer names, dates of birth, Social Security numbers, mailing addresses, telephone numbers, member identification, financial information, and medical claims information. According to Defendants' spokesman Kevin Cane, some customers' credit card information was also compromised. This breach is the result of Defendants' failure to implement cyber security measures commensurate with the duties it undertook by storing vast quantities of sensitive personal data.

6. Many of the affected individuals are children. As explained in more detail below, the danger of identity theft is even graver where children are concerned. To guard against these harms, responsible companies must provide services tailored to the unique challenges presented by child identity theft. Credit monitoring services do little to address the needs of a population with no credit to monitor.

7. Further, and to compound the harm, Defendants knew about the security breach for over one month before they publicly disclosed the incident. Indeed, Defendants have acknowledged that it first learned that their system was compromised on August 5, 2015. They did nothing to warn their customers for the next four weeks.

8. Defendants have yet to fully and accurately inform those affected of the scope of the compromise or the nature of the risks associated with identity theft. It is not clear how many victims Defendants thus far notified, but the companies estimates they

will not complete the notification process until November 9, 2015. This is unacceptable. In a data breach situation, it is incumbent upon the breached company to provide accurate and complete information to those at risk so they may immediately move to protect themselves and their families from further harm. Moreover, the Health Insurance Portability and Accountability Act (HIPAA) requires that Excellus provide notice to those affected without unreasonable delay and no later than 60 days after discovery of a breach. *See* 45 C.F.R. § 164.404.

9. In short, Defendants breached their duty to protect and safeguard its customers' personal, health, and financial information and to take reasonable steps to contain the damage caused where any such information was compromised.

10. Plaintiffs Matthew Fero and Shirley Krenzer, current customers of Defendants, and Erin O'Brien, a former customer of Defendants, therefore bring this action for themselves and on behalf of all persons similarly situated whose personal information was stored by Defendants and compromised as a result of Defendants' failure to safeguard that information. Because Defendants failed in its duty to protect the information of more than 10 million individuals, it must stand to account before the law.

PARTIES

11. Matthew Fero is a citizen of the State of New York and resides in the City of Rochester. Mr. Fero is currently insured under an Excellus policy. To the best of his knowledge, he has been a policyholder for at least nine years. As set forth in more detail below, Mr. Fero has suffered harm because he and his children's personal and health information was compromised when Defendants' cyber security systems were breached

beginning in and around December 2013 and he has spent and will spend time and money safeguarding himself and his family from this fraud.

12. Shirley Krenzer is a citizen of the State of New York and resides in the Town of Spencerport. Mrs. Krenzer is currently insured under an Excellus policy. She has been a policyholder for approximately 30 years and has had her current policy since approximately 2000. As set forth in more detail below, Mrs. Krenzer has suffered harm because her personal and health information is compromised when Defendants' cyber security systems were breached beginning in and around December 2013 and she has spent and will spend time and money safeguarding herself from this fraud.

13. Erin O'Brien is a citizen of the State of South Carolina and resides in the City of Charleston. At the time of the data breach until April 2015, Ms. O'Brien was insured under an Excellus policy through her employer. As set forth in more detail below, Ms. O'Brien has suffered harm because her personal and health information was compromised when Defendants' cyber security systems of Excellus were breached beginning in and around December 2013 and she has spent and will spend time and money safeguarding herself from this fraud.

14. Upon information and belief, defendant Lifetime is a New York domestic not-for-profit corporation registered with the New York Department of State to do business in New York. Lifetime's headquarters are located at 165 Court Street, Rochester, New York 14647.

15. Upon information and belief, Lifetime is the parent and/or holding corporation of a $6.6 billion family of companies known as The Lifetime Healthcare

Companies that finances and delivers health care in New York State, as well as long term care nationwide.

16. Upon information and belief, defendant Excellus is a New York domestic not-for-profit corporation registered with the New York Department of State to do business in New York and organized under Article 43 of the New York State Insurance Law. Excellus' headquarters are located at 165 Court Street, Rochester, New York 14647.

17. Upon information and belief, Excellus operates as a subsidiary of Lifetime and is a licensee of the Blue Cross and Blue Shield Association.

18. Upon information and belief, Lifetime is the sole member of Excellus.

19. Upon information and belief, Excellus is the primary health care provider in upstate New York State, and maintains four regional headquarters in Rochester, Syracuse, Elmira, and Utica, New York. Excellus also maintains additional field offices in Watertown, Binghamton, Oneonta, and Plattsburgh, New York.

20. Upon information and belief, Excellus is the parent of two health maintenance organizations (HMOs) in the New York State Health Insurance Program: Blue Choice and HMO Blue. In addition, Excellus maintains relationships with several Lifetime affiliates, including Lifetime Benefit Solutions, Lifetime Care, Lifetime Health Medical Group, The MedAmerica Companies, and Univera Healthcare.

21. Upon information and belief, Lifetime exercises complete domination over Excellus such that there is no essential difference between the two entities with respect, *inter alia*, to the December 2013 data breach. For example, defendants released a single Annual Financial Report in 2013 and 2014, which shows that the Defendants' high

level employees, including the CEO and vice presidents, as well as the Board of Directors are identical.[4]

22. Defendants have a net income of $24,190,000 in 2014 and $52,557,000 in 2013 according to their 2014 Annual Financial Report.

23. Lifetime and Excellus are collectively referred to as "Defendants" in this Complaint.

JURISDICTION AND VENUE

24. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because Plaintiff Erin O'Brien and upon information and belief members of the proposed Plaintiff Class are citizens of states different from Defendants' home state, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

25. This Court has personal jurisdiction over Excellus because Excellus is organized and incorporated under New York law, licensed and registered to do business in New York, regularly conducts business in New York, and has its headquarters in Rochester, New York.

26. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Excellus and Lifetime reside in this district and regularly conduct business in this district, a substantial part of the events or omissions giving rise to these claims occurred in this district, and Excellus and Lifetime have caused harm to class members residing in this district.

---

[4] *See* The "Limetime Healthcare Companies/Excellus Healthplan, Inc." list of management and Board of Directors, *available at* http://www.lifethc.com/download/files/LTHC-2014AnnualReportFinancials.pdf, p. 38 (last visited Sept. 18. 2015)

FACTUAL BACKGROUND

Defendants Collect and Store Significant Quantities of Customer Data

27. Defendants are one the largest healthcare providers in New York State and, upon information and belief, insure approximately two million individuals in upstate New York alone.

28. Defendants understand that their customers place a premium on privacy. Thus, Excellus provides each of its customers with a notice of privacy practices.[5] It also dedicates a section of its website to explain its privacy and data collection policies.[6]

29. Excellus's notice of privacy practices assures its customers that Excellus is "committed to safeguarding" its customers' "protected health information," and states that it is "required by applicable federal and state laws to maintain the privacy" of personal customer information. The Excellus notice further warrants that it will not provide any nonpublic information without individual consent. Nonpublic information is

---

[5] *See* Excellus Privacy Practices, *available at* https://www.excellusbcbs.com/wps/wcm/connect/1f5e6e27-7bef-411f-bc07-8d38d7e7df7a/Privacy+Notice+-+Excellus+-+Commercial.pdf?MOD=AJPERES&CACHEID=1f5e6e27-7bef-411f-bc07-8d38d7e7df7a (last visited Sept. 17, 2015).

[6] *See* Excellus Website Privacy Policies, *available at* https://www.excellusbcbs.com/wps/portal/xl/!ut/p/b1/jY_LDoIwEEW_hS_odFLbsgSBAkUkoES6MSyMIeGxMX6_kLgwEIGzm8w9k7nEkEocuESKgpMbMX39bp71qxn6up1mw--Xa84SESKcj5JCpJmPzHER1CRUvwEVZQIiViaFLTIERvf5KuaFF9sud9kJeOxhBl_2-fAHZ90fz8_-XwbWfE03fD3rL_MwGNda-ZgmABrn_jKw0T8Nh-5BOtMGE9KxrA8AB-NA/dl4/d5/L2dJQSEvUUt3QS80SmtFL1o2X1RVUjRMN0gyMDhSSEYwSUtLR0UyTkwwMFU2/ (last visited Sept. 17, 2015). The privacy section of Excellus's website is substantially similar to the printed notice of privacy practices provided to each Excellus customer.

defined as, *inter alia*, "names, member identification number, social security number, addresses, type of health care benefits, payment amounts, etc."[7]

30. Excellus's notice of privacy practices explains that it collects most personal and health information directly from its insureds. In addition, Excellus states that it may collect information from third parties such as employers, other healthcare providers, and state and federal agencies.

31. Excellus stresses that its policy is to keep all information about its insured confidential unless required by law to disclose it. Thus, Excellus explains that its employees must sign and follow a code of conduct and complete a privacy training program; Excellus maintains a privacy oversight committee; and it employs a "security coordinator" to detect and prevent data breaches.[8]

32. The Website Privacy Policy on Excellus's website adds to these assurances; it stresses that Excellus is "committed to protecting any personal information" that individuals provide. What is more, Excellus stresses that its collection of personal health and financial information is required in order to obtain its healthcare services. Excellus notes, however, that its customers need not worry: "Personally Identifiable Information you provide to Excellus BlueCross BlueShield via this website

---

[7] Excellus Privacy Practices, *available at* https://www.excellusbcbs.com/wps/wcm/connect/1f5e6e27-7bef-411f-bc07-8d38d7e7df7a/Privacy+Notice+-+Excellus+-+Commercial.pdf?MOD=AJPERES&CACHEID=1f5e6e27-7bef-411f-bc07-8d38d7e7df7a (last visited Sept. 17, 2015).

[8] *Id.*

will only be used for the express purpose of your disclosure to us, unless otherwise described herein."[9]

33. The statements on Excellus's website and in its notice of privacy practices make clear that Defendants are aware of the importance their customers place on privacy, as well as their duty to safeguard the personal and health information that their customers supply to them, and to promptly notify their customers if their information is compromised.

The Defendants' Breach

34. In December 2013, hackers gained access to Defendants' data systems. For the next twenty months, these intruders operated undetected in the Defendants' system.

35. Defendants did not discover that hackers were in its system until August 5, 2015.

36. Based on the message from the President and CEO on Defendants' data breach information websites, http://www.excellusfacts.com/ and http://www.lifethcfacts.com/, hackers had access to highly sensitive personal, health, and financial information, including names, dates of birth, Social Security numbers, mailing addresses, telephone numbers, member identification, financial payment information, and

---

[9] [9] *See* Excellus Website Privacy Policies, *available at* https://www.excellusbcbs.com/wps/portal/xl/!ut/p/b1/jY_LDoIwEEW_hS_odFLbsgSBAkUkoES6MSyMIeGxMX6_kLgwEIGzm8w9k7nEkEocuESKgpMbMX39bp71qxn6up1mw--Xa84SESKcj5JCpJmPzHER1CRUvwEVZQIiViaFLTIERvf5KuaFF9sud9kJeOxhBl_2-fAHZ90fz8_-XwbWfE03fD3rL_MwGNda-ZgmABrn_jKw0T8Nh-5BOtMGE9KxrA8AB-NA/dl4/d5/L2dJQSEvUUt3QS80SmtFL1o2X1RVUjRMN0gyMDhSSEYwSUtLR0UyTkwwMFU2/ (last visited Sept. 17, 2015).

medical insurance claims information. Some of this financial payment information included credit card numbers.

37. Although the information in Defendants' system was encrypted, this traditional safeguard was largely irrelevant because the hackers went undetected for so long. Indeed, Defendants have acknowledged that because hackers gained access to their network, they would have been able to circumvent its encryption, likely accessing decryption keys available to administrators on the system.

38. Indeed, Adam Kujawa, malware intelligence leader at cybersecurity firm Malwarebytes, recently stated, "With an attack of this magnitude, being done over the course of more than a year, cybercriminals probably stole information by simply copying and pasting it from its unencrypted form on the secure network to their own systems, or utilizing built-in tools to parse the information for the most valuable data."[10]

39. On or about September 9, 2015, Defendants publicly disclosed the breach, and stated that between 10 and 10.5 million individuals were affected. The affected individuals include not only past and current Excellus policyholders, but also those insured through Defendants' affiliates. Upon information and belief, members of the BlueCross BlueShield network who received treatment 31 county upstate New York service area of Excellus are also likely affected.

40. When it disclosed the breach, Defendants' President and CEO Christopher Booth publicly posted a message online at http://www.excellusfacts.com/ and http://www.lifethcfacts.com/. In that message, Mr. Booth stated that safeguarding the

[10] *Hackers Home In On Health, Education, Government Sectors,* http://www.technewsworld.com/story/82495.html (last visited Sept. 16, 2015).

privacy of its customers' personal information was a "top priority" and that Defendants' "make[s] every effort" to protect the information of its insureds.[11]

41. Mr. Booth's statement informed breach victims that Defendants' would offer two years of free credit monitoring through third-party provider Kroll, Inc., and that it remained "committed" to ensuring that victims "get the tools and assistance" needed for protection.[12]

42. Defendants assured the public that all affected individuals will receive a letter on or before November 9, 2015, notifying them of the breach.

43. Defendants did not explain why it waited almost one month before disclosing the breach.

44. Some individuals, including Plaintiffs Matthew Fero and his family and Shirley Krenzer, began receiving these letters on September 14, 2015. In the letters, Defendants' President and CEO urged affected individuals to take steps to protect themselves, including enrolling in credit monitoring services provided by Kroll, conducting regular reviews of Explanation of Benefits statements received from Excellus, and independently monitoring bank and credit statements.

45. Remarkably, although Defendants knows that many of the affected victims are minors, it is not clear exactly what type of protection is being offered to minor victims. The letter to Plaintiff Matthew Fero's children states, "we have secured the services of Kroll to provide identity theft protection at no cost to your child for two years" and that those services include "Identity Theft Consultation and Restoration." The sent to the parents, however, and other adult victims specifically states, "To receive credit

---

[12] *Id.*

services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file." Thus, it appears that Defendants are only offering to provide restoration services for two years should a problem arise for the minor victims. This rings hollow with no monitoring provided to detect the problem.

46. The letter sent by Defendants' President and CEO does not even provide guidance to parents seeking to protect affected minors. It simply states that parents can call a toll free number if they have any questions..

47. On September 15, 2015, the New York State Public Employees Federation issued a warning of its own. After advising its membership about the details of the breach, the Public Employees Federation set forth a list of safeguards victims may take to protect themselves. Those safeguards include: enrolling in credit monitoring; monitoring credit reports; placing a fraud alert with each of the three major credit agencies; and placing a credit freeze on one's credit report.[13]

48. Plaintiff Matthew Fero signed himself and his wife up for the free, two-year credit monitoring offered by Defendants through Kroll. Defendants have not provided any identity theft protection for Plaintiff Matthew Fero's two minor children nor have they provided him any information on how to protect his children from identity theft. Plaintiff Matthew Fero will have to look into ways to do this himself and will have to pay money to do so.

---

[13] New York State Public Employees Federation, Excellus BlueCross BlueShield (Excellus BCBS) Data Breach (Sept. 15, 2015), http://www.pef.org/wp-content/uploads/2015/08/Excellus-Security-Breach-Memo.pdf.

49. Plaintiff Shirley Krenzer signed herself and her husband up for the free, two-year credit monitoring offered by Defendants.

50. Plaintiff Erin O'Brien signed herself up for the free, two-year credit monitoring offered by Defendants.

The Value of the Stolen Data

51. The breadth of data compromised in the Excellus/Lifetime hack is astounding and is therefore particularly valuable to thieves. The compromised data leaves Defendants' customers especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more. As Pam Dixon, executive director of the World Privacy Forum, stated: "When someone has your clinical information, your bank account information, and your Social Security number, they can commit fraud that lasts a long time. Th[is] kind of identity theft . . . is qualitatively and quantitatively different than what is typically possible when you lose your credit card . . . ."[14]

52. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

53. The Social Security Administration has warned that identity thieves can use an individual's Social Security number and good credit score to apply for additional

[14] Premera Hack: What Criminals Can Do With Your Healthcare Data, Christian Science Monitor, Jaikumar Vijayan, Mar. 20, 2015, *available at* http://www.csmonitor.com/World/Passcode/2015/0320/Premera-hack-What-criminals-can-do-with-your-healthcare-data (last visited Sept. 16, 2015).

credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.[15]

54. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

55. The incidence of fraudulent tax filings has increased dramatically over the past years. The IRS paid an estimated $5.2 billion in tax refunds obtained from identity theft in 2013, while it prevented an additional $24.2 billion in fraudulent transfers the same year.[16]

56. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

57. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks

---

[15] Social Security Administration, Identity Theft and Your Social Security Number, http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Sept. 16, 2015).

[16] FBI Probes Rash of Fraudulent State Tax Returns Filed Through Turbo Tax, LA Times, Shan Li, Feb. 11, 2015, *available at* http://www.latimes.com/business/la-fi-turbotax-fbi-20150212-story.html (last visited Sept. 16, 2015).

are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[17]

58. The danger of identity theft is compounded when a minor's Social Security number and personal information is compromised. Whereas adults can periodically monitor their own credit reports, minors typically have no credit to monitor. Thus, it can be difficult to safeguard against fraud because a minor cannot simply place an alert on his or her credit report. Nor can a minor "freeze" his or her credit report in most states. In order to "freeze" a minor's credit report, a report must exist. In some instances, and with the assistance of the credit reporting bureaus, a parent may create a credit report for the purpose of freezing it. This process is not well known to most consumers and is administratively difficult. Premium identity protection services, however, typically offer counseling to identity theft victims to navigate them through this process. Excellus has not offered victims any counseling to guide them through the steps required to adequately protect the credit of a minor child.

59. Another danger, according to the publisher of *Privacy Journal*, Robert Ellis Smith, is that thieves use stolen Social Security numbers to obtain medical care in someone else's name.[18]

60. Medical identity fraud affected 2.3 million people in 2014—an increase of 21% over the previous year. A study by the Ponemon Institute concluded that victims of

---

[17] Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR, Brian Naylor, Feb. 9, 2015, *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Sept. 16, 2015).

[18] Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR, Brian Naylor, Feb. 9, 2015, *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Sept. 16, 2015).

such fraud spend an average of $13,500 to resolve problems stemming from medical identity theft.[19]

61. Moreover, fraudulent medical treatment can have non-financial impacts as well. Deborah Peel, executive director of Patient Privacy Rights, has described scenarios in which an individual may be given an improper blood type or administered medicines because his or her medical records contain information supplied by an individual obtaining treatment under a false name.[20]

62. In the Excellus/Lifetime hack, customer clinical information was compromised. This means any information contained in an individual's medical records is subject to disclosure or, worse, medical blackmail.

63. The Ponemon Institute study concluded that a victim of medical identity theft typically does not learn of the fraudulent treatment for three months. To guard against medical identity fraud, cyber security experts suggest that individuals routinely obtain the most recent copy of their medical records and inspect them for discrepancies. Excellus's proposed customer solutions do nothing to address the problem of medical identity theft, and Excellus has done nothing to advise its customers how to obtain and inspect their medical records for fraud to comport with best practices identified by security experts.

---

[19] Ponemon Institute LLC, Fifth Annual Study on Medical Identity Theft 2 (Sept. 2015), *available at* http://assets.fiercemarkets.com/public/healthit/ponemonmedidtheft2015.pdf (last visited Sept. 16, 2015).

[20] *See* 2015 is Already the Year of the Health-Care Hack—and It's Only Going to Get Worse, Wash. Post, Andrea Peterson, Mar. 20, *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/ (last visited Sept. 16, 2015).

64. The victims of the Excellus/Lifetime data breach are also now at heightened risk of health insurance discrimination. Stolen medical and clinical information may be improperly disclosed for use to discriminate in the provision of healthcare to insureds and prospective insureds. Individuals risk denial of coverage, improper "redlining," and denial or difficulty obtaining disability or employment benefits because information was improperly disclosed to a provider. This risk is pervasive and widespread. Indeed, most states maintain government agencies that investigate and combat health insurance discrimination, as does the Office for Civil Rights in the Department of Health and Human Services.

65. The personal information compromised in the Excellus/Lifetime data breach is significantly more valuable than the credit card information that was compromised in the large retailer data breaches at Target and Home Depot. Victims affected by the retailer breaches could avoid much of the potential for future harm by cancelling credit or debit cards and obtaining replacements. The information compromised in the Excellus breach is difficult, if not impossible, to change—Social Security number, name, date of birth, employment information, income data, etc.

66. These data, as one would expect, demand a much higher price on the black market. Martin Walter, senior director at cyber security firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[21]

[21] Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, IT World, Tim Greene, Feb. 6, 2015, *available at* http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Sept. 16, 2015).

67. This estimate may be low. A recent PriceWaterhouseCoopers report stated that an identity theft kit containing health insurance credentials can be worth up to $1,000 on the black market, while stolen credit cards may go for $1 each.

68. Further, a report released by the Ponemon Institute in late February concluded that 65% of medical identity theft victims pay more than $13,500 out of pocket to resolve identity theft issues and spend 200 hours with insurers and providers to secure their credentials, and check the accuracy of their personal information, invoices, and e-health records.[22]

69. When it disclosed the breach, Excellus/Lifetime announced that it would offer free credit monitoring services for two years. While this gesture is not worthless, security blogger Brian Krebs has explained that "the sad truth is that most services offer little in the way of real preventative protection against the fastest-growing crime in America [identity theft]."[23] Credit monitoring services, in other words, may inform individuals of fraud after the fact, but do little to thwart fraud from occurring in the first instance.

70. Further, the credit monitoring service offered by Defendants fail to meet the industry standard for credit monitoring services. Defendants' chosen service, provided by Kroll, only monitors a victim's credit at one of the three major credit bureaus (but not the other two). For example, Kroll will monitor a victim's credit at Trans Union but not Experian or Equifax. If a fraudster applies for a credit line that is not reported to

---

[22] Ponemon Institute, 2014 Fifth Annual Study on Medical Identity Theft, http://medidfraud.org/2014-fifth-annual-study-on-medical-identity-theft/.

[23] Brian Krebs, Are Credit Monitoring Services Worth It?, Krebs on Security, Mar. 4, 2014, http://krebsonsecurity.com/2014/03/are-credit-monitoring-services-worth-it/ (last visited Sept. 16, 2015).

Trans Union, the Kroll credit monitoring will not detect it. Given the severity of this breach, Defendants should be providing a service that will monitor credit at each of the three major reporting agencies.

71. Further, and as described above, Defendants are not offering credit monitoring for any victim under the age of eighteen nor providing any information on how to protect minor victims from identity threat even though it knows and understands that many of the victims of this incident are minors. Credit monitoring services that make no attempt to protect the identities and credit of minors and only offer restoration services should a problem arise are not a reasonable under the circumstances..

72. The implications of the Excellus/Lifetime data breach are indeed serious. But these implications were known *ex ante*. Defendants should have—and could have—done more to fulfill its duty to safeguard the data with which their customers entrusted it.

The Healthcare and Health Insurance Industry—Including Defendants—Is On Notice That It Is A Target of Cyber Thieves

73. Healthcare and health insurance companies, including Defendants, are well aware that they are the target of cyber thieves, yet the industry has failed to implement the cyber security reforms implemented across other industries.

74. Martin Walter, senior director at RedSeal, has stated that companies in the healthcare industry "in comparison spend significantly less on security, making them

tentatively easier targets."[24] Cyber security analysts generally believe that the healthcare industry lags far behind other industries when it comes to cyber security.[25]

75. Dave Kennedy, chief executive of information security firm TrustedSEC, has explained that healthcare organizations are targets because they maintain troves of data with significant resale value in black markets and their security practices are less sophisticated than other industries. "Health organizations sometimes rely on legacy systems, and some have not invested in cybersecurity at a rate that matches the urgency of the threats they face. The medical industry is years behind other industries when it comes to security."[26]

76. The cybersecurity firm WhiteHat recently reported that in the healthcare industry, only 24% of known security flaws are fixed at any given time.[27]

77. Furthermore, the events of 2014 and 2015 alone should have placed Defendants on notice of the need to improve its cyber security systems. In August 2014, Community Health Systems, the second largest for-profit hospital chain in the United

---

[24] Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, IT World, Tim Greene, Feb. 6, 2015, *available at* http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Sept. 16, 2015).

[25] *See* Data Breach at Anthem May Forecast a Trend, New York Times, Reed Abelson & Julie Creswell, Feb. 6, 2015, *available at* http://www.nytimes.com/2015/02/07/business/data-breach-at-anthem-may-lead-to-others.html (last visited Sept. 16, 2015).

[26] *See* 2015 is Already the Year of the Health-Care Hack—and It's Only Going to Get Worse, Wash. Post, Andrea Peterson, Mar. 20, *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/ (last visited Sept. 16, 2015).

[27] Premera Hack: What Criminals Can Do With Your Healthcare Data, Christian Science Monitor, Jaikumar Vijayan, Mar. 20, 2015, *available at* http://www.csmonitor.com/World/Passcode/2015/0320/Premera-hack-What-criminals-can-do-with-your-healthcare-data (last visited Sept. 16, 2015).

States, was hacked and the Social Security numbers of 4.5 million customers were stolen. This prompted a "flash warning" by the FBI to entities in the healthcare industry warning it had observed "malicious actors targeting health care related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[28]

78. Earlier in the year, over 12,000 patients' records were compromised when hackers gained access to the accounts of employees of Centura Health Systems of Colorado Springs. This event was preceded by a breach at Texas's St. Joseph Health System compromising 405,000 patient records. In spite of these industry warnings, Premera took insufficient steps to ensure its IT systems had not been breached until January 2015—nearly nine months after hackers gained access to its system.

79. In early 2015, Anthem, Inc. disclosed that its systems were hacked and the personal information of 80 million individuals was compromised. Shortly thereafter, Premera Blue Cross, a healthcare provider in the Pacific Northwest, announced that its systems were also hacked and 11 million individuals were compromised.

80. The history of cyber security breaches in the industry, and the warnings that are now all but ubiquitous, have placed companies operating in the industry on notice of the duty to safeguard customers' personal, health, and financial information. If anything, this history of failure should spur greater efforts to implement top-of-the-line cyber security measures that exceed the industry standard. Indeed, customers expect that healthcare companies will take every precaution to safeguard their personal information.

---

[28] FBI Warns Healthcare Firms They Are Targeted By Hackers, Reuters, Aug. 20, 2014, *available at* http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820 (last visited Sept. 16, 2015).

The unfortunate reality, as Les Funtleyder, a health care portfolio manager, observed, is that "health care has been very slow to adopt almost every technological advance. Right now, a lot of health care companies are sitting ducks."[29]

CLASS ACTION ALLEGATIONS

81. Plaintiffs bring this lawsuit as a class action on their own behalf and on behalf of all other persons similarly situated as members of the proposed Class pursuant to Federal Rules of Civil Procedure 23(a) and (b)(3) and/or (b)(2). This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of those provisions.

82. The proposed nationwide class is defined as:

> **Nationwide Class**
> All persons in the United States who are or were insured by Excellus, Lifetime and/or its affiliates as of August 5, 2015, and all persons in the United States who were not insured by Excellus, Lifetime and/or its affiliates as of August 5, 2015 but who are or were Blue Cross Blue Shield customers who received medical treatment in the 31 county upstate New York service area of Excellus on or before August 5, 2015.

83. Plaintiffs also bring this action on behalf of a New York State Class, defined as:

> **New York Class**
> All persons who reside in New York and who are or were insured by Excellus, Lifetime and/or its affiliates as of August 5, 2015, and all persons who reside in New York who were not insured by Excellus, Lifetime and/or its affiliates as of August 5, 2015 but who are or were BlueCross BlueShield customers and who received medical treatment in the 31 county upstate New York service area of Excellus on or before August 5, 2015.

[29] Indianapolis Business Journal, *Anthem's IT System Had Cracks Before Hack*, J.K. Wall, Feb. 14, 2015, http://www.ibj.com/articles/51789-anthems-it-system-had-cracks-before-hack (last visited Sept. 16, 2015).

84. Excluded from the Class are: (1) Defendants, any entity or division in which Defendants have a controlling interest, and their legal representatives, officers, directors, assigns, and successors; (2) the Judge to whom this case is assigned and the Judge's staff; and (3) governmental entities. Plaintiffs reserve the right to amend the Class definition if discovery and further investigation reveal that the Class should be expanded, divided into subclasses or modified in any other way.

Numerosity

85. Although the exact number of class members is uncertain and can be ascertained only through appropriate discovery, the number is great enough such that joinder is impracticable. The disposition of the claims of these class members in a single action will provide substantial benefits to all parties and to the Court. Class members are readily identifiable from information and records in Excellus's possession, custody, or control.

Typicality

86. Plaintiffs' claims are typical of the claims of the Class in that Plaintiffs, like all class members, entrusted personal and health information to Defendants in connection with healthcare services or treatment. Plaintiffs, like all class members, have been damaged by Defendants' conduct in that their personal and health information, including their Social Security number and clinical information, have been compromised by Defendants' failure to fulfill their duties under the law. Further, the factual bases of Defendants' misconduct are common to all class members and represent a common thread of misconduct resulting in injury to all class members.

Adequate Representation

87. Plaintiffs will fairly and adequately represent and protect the interests of the Class. Plaintiffs have retained counsel with substantial litigation experience, including experience in prosecuting consumer and data breach class actions, and therefore Plaintiffs' counsel is also adequate under Rule 23.

88. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the Class and have the financial resources to do so. Neither Plaintiffs nor her counsel has interests adverse to those of the Class.

Predominance of Common Issues

89. There are numerous questions of law and fact common to Plaintiffs and the class members that predominate over any question affecting only individual class members. The answers to these common questions will advance resolution of the litigation as to all class members. These common legal and factual issues include:

a. Whether Defendants owed a duty to Plaintiffs and members of the Class to take reasonable measures to safeguard their personal information;

b. Whether Defendants knew or should have known that its cyber security systems were vulnerable to attack;

c. Whether Defendants' breach of a legal duty caused its cyber security systems to be compromised, resulting in the loss and/or potential loss of over 10 million individual files;

d. Whether Defendants owed a duty to Plaintiffs and members of the Class to provide timely and adequate notice of the Defendants' data breach

and the risks posed thereby, and whether Defendants' notice was, in fact, timely;

e. Whether it was reasonable for Defendants to maintain the personal, health, and financial information of members of the Excellus Treatment Subclass and, if so, whether Defendants had a duty to these Class members to use reasonable means to safeguard their personal, financial, and health information; and

f. Whether Plaintiffs and class members are entitled to recover actual damages, statutory damages, and/or punitive damages.

Superiority

90. Plaintiffs and members of the Class have all suffered and will continue to suffer harm and damages as a result of Defendants' unlawful and wrongful conduct. A class action is superior to other available methods for the fair and efficient adjudication of this controversy.

91. Absent a class action, most class members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy at law. Further, without class litigation, class members will continue to incur damages and Defendants are likely to repeat its misconduct.

92. Class treatment of common questions of law and fact is also a superior method to multiple individual actions or piecemeal litigation in that class treatment will conserve the resources of the courts and the litigants, and will promote consistency and efficiency of adjudication.

CAUSES OF ACTION

FIRST CLAIM FOR RELIEF

Negligence

93. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

94. Plaintiffs bring this Claim on behalf of the Nationwide Class under New York law.

95. In the alternative, Plaintiffs bring this Claim on behalf of the New York Class under New York law.

96. Defendants required Plaintiffs and class members to submit non-public personal and health information in order to acquire coverage under a health insurance policy and/or receive treatment in the Blue Cross Blue Shield network while in New York. In addition, Defendants required those who received treatment at its upstate New York facilities to submit non-public personal and health information in order to receive treatment. Defendants collected and stored this data. It therefore assumed a duty of care to use reasonable means to secure and safeguard this personal and health information, to prevent disclosure of the information, and to guard the information from theft. Defendants' duty included a responsibility to implement a process by which it could detect a breach of its security systems in a reasonably expeditious period of time.

97. Defendants' duty arises from the common law, as well as principles embodied in New York state law, and HIPAA.

98. Defendants breached their duty of care by failing to secure and safeguard the personal and health information of Plaintiffs and the Class. Defendants negligently

maintained systems that it knew were vulnerable to a security breach. Further, the systems maintained by Defendants were so poor that hackers were able to remain undetected in Defendants' systems for approximately twenty months, subverting any benefits Defendants may have reaped by encrypting its data.

99. Given the risks associated with data theft, Defendants also assumed a duty of care to promptly and fully notify and inform individuals affected by a breach should their personal information be compromised and/or stolen.

100. Defendants breached this duty of care when it unreasonably waited over four weeks to notify the Class that its security systems had been breached. Defendants learned of the breach on August 5, 2015, yet said nothing to notify those affected for over four weeks.

101. Plaintiffs and the Class have suffered harm as a result of Defendants' breach. The personal and health information of Plaintiffs and the Class have been exposed, subjecting each member of the Class to identity theft, credit and bank fraud, Social Security fraud, tax fraud, medical identity fraud, and myriad other varieties of identity fraud.

102. Plaintiffs and the Class have suffered monetary damages and will continue to be injured and incur damages in the future both in an effort to protect themselves and to remedy acts of fraudulent activity. Plaintiffs and the Class have suffered and/or are reasonably likely to suffer theft of personal and health information; costs associated with prevention, detection, and mitigation of identity theft and/or fraud; costs associated with time spent and productivity loss resulting from addressing the consequences of fraud in

any of its myriad forms; and damages from the unconsented exposure of personal and health information due to this breach.

SECOND CLAIM FOR RELIEF

Negligence Per Se

103. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

104. Plaintiffs bring this Claim on behalf of the Nationwide Class under New York law.

105. In the alternative, Plaintiffs bring this Claim on behalf of the New York Class under New York law.

106. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Defendants had a duty to secure and safeguard the personal information of its customers. Defendants acknowledged this duty to its customers in its Notice of Privacy Practices, and warranted that it would comport with its duties under HIPAA.

107. Defendants violated HIPAA by failing to secure and safeguard the personal information entrusted to it by Plaintiffs and the Class, and by failing to implement protections against "reasonably anticipated threats," 45 C.F.R. § 164.306.

108. Defendants' failure to comply with HIPAA and regulations promulgated thereto constitutes negligence per se.

109. As a result of Defendants' negligence per se, Plaintiffs and the Class have suffered monetary damages and will continue to be injured and incur damages in the future both in an effort to protect themselves and to remedy acts of fraudulent activity. Plaintiffs and the Class have suffered and/or are reasonably likely to suffer theft of

personal and health information; costs associated with prevention, detection, and mitigation of identity theft and/or fraud; costs associated with time spent and productivity loss resulting from addressing the consequences of fraud in any of its myriad forms; and damages from the unconsented exposure of personal and health information due to this breach.

THIRD CLAIM FOR RELIEF

Bailment

110. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

111. Plaintiffs bring this Claim on behalf of the Nationwide Class under New York law.

112. In the alternative, Plaintiffs bring this Claim on behalf of the New York Class under New York law.

113. Plaintiffs and the Class delivered personal and health information to Defendants for the exclusive purpose of obtaining health insurance and/or medical treatment.

114. By delivering their personal and health information to Defendants, Plaintiffs and the Class intended and understood that Defendants would adequately safeguard their personal and health information from being accessed by or disclosed to unauthorized persons.

115. Defendants accepted possession of the personal and health information of Plaintiffs and the Class for the purpose of providing health insurance to Plaintiffs and the Class.

116. By accepting possession of the personal and health information of Plaintiffs and the Class, Defendants understood that Plaintiffs and the Class expected Defendants to adequately safeguard their information. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

117. During the bailment, Defendants owed a duty to Plaintiffs and the Class to exercise reasonable care, diligence, and prudence in protecting their personal and health information.

118. Defendants breached their bailment and their duty of care by failing to take appropriate measures to safeguard and protect the personal and health information of Plaintiffs and the Class. This breach resulted in the unlawful and unauthorized access to and misuse of the personal and health information of Plaintiffs and the Class.

119. Defendants further breached their bailment and their duty to safeguard the personal and health information of Plaintiffs and the Class by failing to timely and completely notify Plaintiffs and the Class that their private information was compromised as a result of the breach.

120. As a result of Defendants' breach, Plaintiffs and the Class have suffered monetary damages and will continue to be injured and incur damages in the future both in an effort to protect themselves and to remedy acts of fraudulent activity. Plaintiffs and the Class have suffered and/or are reasonably likely to suffer theft of personal and health information; costs associated with prevention, detection, and mitigation of identity theft and/or fraud; costs associated with time spent and productivity loss resulting from addressing the consequences of fraud in any of its myriad forms; and damages from the unconsented exposure of personal and health information due to this breach.

FOURTH CLAIM FOR RELIEF

Breach of Contract

121. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

122. Plaintiffs bring this Claim on behalf of the Nationwide Class under New York law.

123. In the alternative, Plaintiffs and the Class bring this Claim on behalf of the New York State Class under New York law.

124. Defendants entered into written contracts with Plaintiffs and the Class in which it agreed to provide a health insurance policy for a fixed period of time in exchange for periodic premium payments.

125. As part of its contractual agreement, Defendants undertook the obligation to maintain the security of its customers' personal and health information. Defendants recognizes this obligation in its notice of privacy practices, where it assures individuals that it will not disclose nonpublic information, and sets forth the measures it takes to ensure patient privacy is maintained.

126. Defendants breached their contractual obligation by failing to safeguard the personal and health information of Plaintiffs and the Class, and by failing to timely notify Plaintiffs and the Class that their personal and health information was compromised by a data breach.

127. In the alternative, and if the Court finds that Defendants did not enter into an explicit contract with Plaintiffs and members of the Class, then Plaintiffs ask that the

Court find that Defendants entered into an implied contract with the Class, and that Defendants violated this implied contract by failing to abide by its privacy warranties.

128. Plaintiffs and the members of the Class and seek actual damages as described herein to be proven at trial, as well as attorneys' fees and costs as permitted by law.

FIFTH CLAIM FOR RELIEF

Breach of Fiduciary Duty

129. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

130. Plaintiffs bring this Claim on behalf of the Nationwide Class under New York law.

131. In the alternative, Plaintiffs bring this Claim on behalf of the New York Class under New York law.

132. Defendants collected and stored highly personal and private information, including health information, belonging to Plaintiffs and members of the Class. Because this information is of a heightened sensitivity and importance, it receives special protection under federal law. Indeed, HIPAA protects all "individually identifiable health information," as well as individual identifiers such as Social Security numbers and medical identification numbers. *See, e.g.*, 45 C.F.R. § 160.103. What is more, HIPAA imposes heightened duties on entities like Defendants that collect and store such information, subjecting them to a range of penalties when protected health information is wrongfully disclosed. *See, e.g.*, 42 U.S.C. §§ 1320d-5, 1320d-6.

133. By virtue of its collection of highly personal information, including health information, and the warranties made in its notice of privacy practices, a fiduciary relationship arose between Defendants and the class members that is actionable at law.

134. By virtue of this fiduciary relationship, Defendants owed Plaintiffs and members of the Class a fiduciary duty to safeguard the personal and health information that it collected and stored; to warn Plaintiffs and the Class when it learned that the security of the collected data may be vulnerable; and to immediately and fully notify Plaintiffs and the Class when it knew that its cyber security systems had been breached. This duty required Defendants to ensure that the interests of Plaintiffs and the Class would be adequately cared for, both before and after the security breach. By virtue of its duty, Defendants owe Plaintiffs and the Class assistance in protecting themselves now that a breach has occurred, not just from financial fraud, but also from medical identity fraud, health insurance discrimination, tax fraud, and other forms of identity fraud described herein.

135. In the event that the Court finds that this Claim may not be raised on behalf of the Nationwide Class, Plaintiffs and the Class bring this Claim on behalf of the New York Class under New York law..

136. As a result of Defendants' breach of its fiduciary duties, Plaintiffs and the Class have suffered actual damages, and prospective damages that are reasonably likely to arise. Defendants have taken insufficient steps to protect the Class from these reasonably likely prospective damages, and Plaintiffs and the Class therefore also request equitable and/or injunctive relief to require Defendants to take steps to prevent the forms of identity fraud alleged herein.

SIXTH CLAIM FOR RELIEF

Deceptive Acts or Practices in Violation of N.Y. General Business Law § 349 et seq.

137. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

138. Plaintiffs bring this Claim on behalf of the Nationwide Class under New York law.

139. In the alternative, Plaintiffs bring this Claim on behalf of the New York Class under New York law.

140. New York General Business Law § 349 ("NYGBL § 349") prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in this state.

141. As one of the largest healthcare providers in New York State, Defendants conducted business, trade or commerce in New York State.

142. In the conduct of its business, trade and commerce, and in its furnishing services in New York State, Defendants' actions were directed at consumers.

143. In the conduct of its business, trade and commerce, and in its furnishing services in New York State, Defendants collected and stored highly personal and private information, including health and financial information, belonging to Plaintiffs and members of the Class.

144. Defendants violated NY GBL § 349, and continue to violate NY GBL § 349, by engaging in the deceptive, misleading, and unlawful acts and practices described in this Complaint.

145. Among other things, Defendants violated NY GBL § 349 by:

a. falsely representing to Plaintiffs and members of the Class that personal, health and financial information provided to Defendants would be safe and secure from theft and unauthorized disclosure;

b. falsely representing to Plaintiffs and members of the Class that they maintained policies and practices sufficient to secure and safeguard this personal, health and financial information;

c. failing to take reasonable means to secure and safeguard this personal, health and financial information to prevent disclosure of the information and guard it from theft;

d. maintaining systems that they knew were vulnerable to a security breach;

e. failing to implement cyber security measures commensurate with the duties they undertook by storing vast quantities of personal, health and financial information;

f. failing to implement a process by which they could detect a breach of its security systems in a reasonably expeditious period of time;

g. learning about the security breach on August 5, 2015, but waiting more than four weeks to disclose publically the security breach; and

h. continuing to collect and maintain personal, health and financial data when they knew or should have known of the security vulnerabilities that were exploited in the data breach.

146. Defendants systematically engaged in these deceptive, misleading, and unlawful acts and practices, to the detriment of Plaintiff and members of the Class.

147. Defendants willfully engaged in such acts and practices, and knew that it violated NYGBL § 349 or showed reckless disregard for whether it violated NYGBL § 349.

148. As a result of Defendants' violations of NYGBL § 349, Plaintiff and members of the Class have been injured and have suffered actual damages, and prospective damages that are reasonably likely to arise.

149. Plaintiff and members of the Class are entitled to actual damages, statutory damages, treble damages, injunctive relief, attorneys' fees and costs and expenses, and any other remedies available under New York law or in equity, for Defendant's violations of NYGBL § 349. *See* N.Y. Gen. Bus. Law § 349(h).

PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and all others similarly situated, request the Court to enter judgment against Defendants as follows:

A. An order certifying the proposed Class designating Plaintiffs as the named representatives of the Class, and designating the undersigned as Class Counsel;

B. An order awarding Plaintiffs and the Class relief, including actual and statutory damages, as well as equitable and/or injunctive relief as requested herein;

C. An injunction ordering Defendants to immediately notify each individual whose personal information was compromised and/or an order awarding Plaintiffs and the Class preliminary or other equitable or declaratory relief as may be appropriate by way of applicable state or federal law as requested herein;

D. Any additional orders or judgments as may be necessary to prevent further unlawful practices and to restore to any person in interest any money or property that may have been acquired by means of the violations;

E. An award of attorneys' fees and costs, as provided by law;

F. An award of pre-judgment interest and post-judgment interest, as provided by law;

G. Leave to amend this Complaint to conform to the evidence produced at trial; and

H. Any other favorable relief as may be available and appropriate under law or equity.

JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of any and all issues in this action so triable of right.

Dated: September 18, 2015

/s/ Hadley L. Matarazzo
Hadley L. Matarazzo (NY Bar No. 437785)
hmatarazzo@faraci.com
Kathryn Lee Bruns (NY Bar No. 2874063)
kbruns@faraci.com
FARACI LANGE, LLP
28 E. Main Street, Suite 1100
Rochester, New York 14614
Tel: (585) 325-5150
Fax: (585) 325-3285

/s/ Robin L. Greenwald
Robin L. Greenwald (*pro hac vice* to be filed)
rgreenwald@weitzlux.com
James J. Bilsborrow (*pro hac vice* to be filed)
jbilsborrow@weitzlux.com
WEITZ & LUXENBERG, P.C.
700 Broadway
New York, New York 10003
Tel: (212) 558-5500
Fax: (646) 293-7937